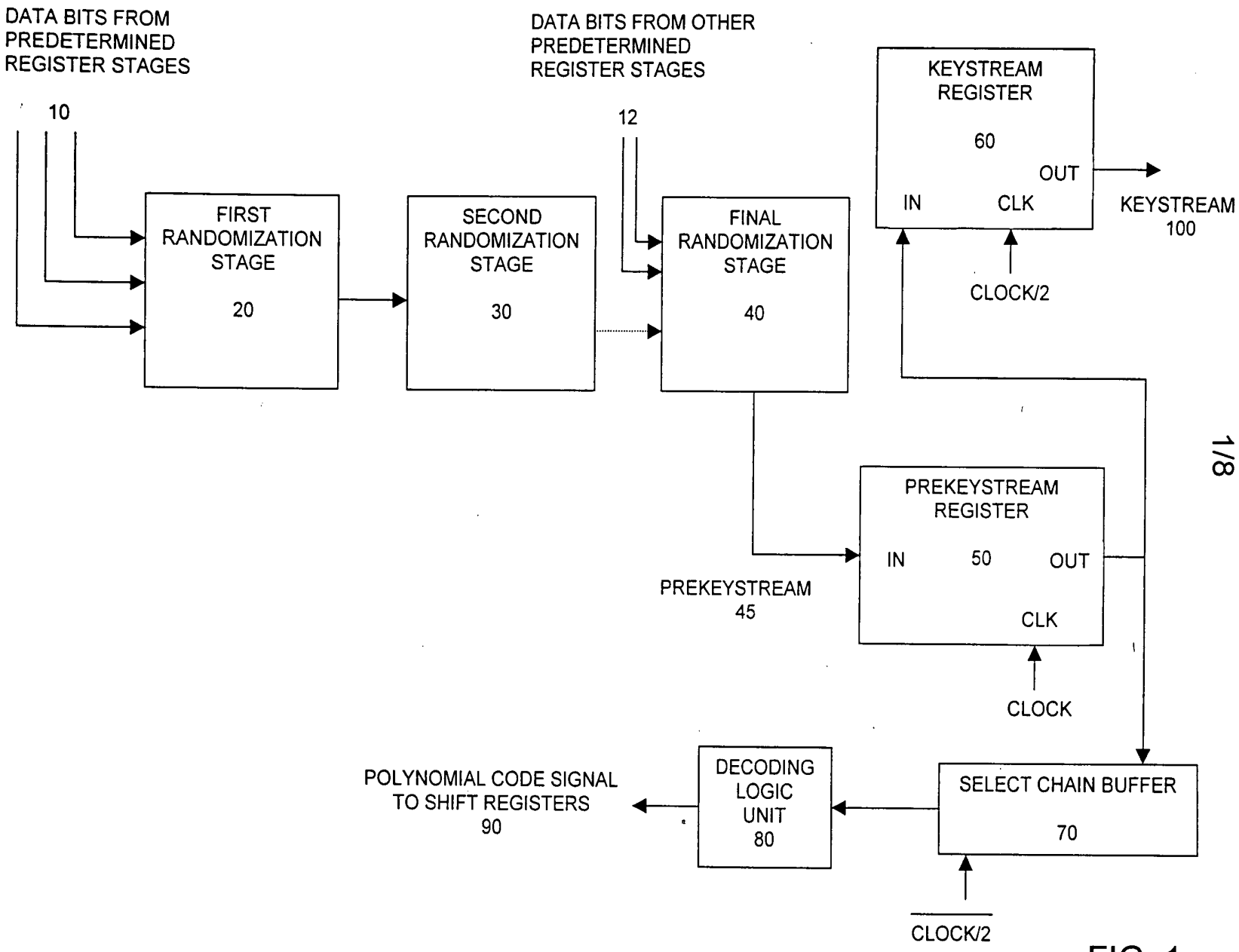
DATA BITS FROM PREDETERMINED REGISTER STAGES
10
DATA BITS FROM OTHER PREDETERMINED REGISTER STAGES
12
FIRST RANDOMIZATION STAGE
20
SECOND RANDOMIZATION STAGE
30
FINAL RANDOMIZATION STAGE
40
KEYSTREAM REGISTER
60
IN
CLK
OUT
KEYSTREAM
100
CLOCK/2
PREKEYSTREAM REGISTER
IN
50
OUT
CLK
PREKEYSTREAM
45
CLOCK
POLYNOMIAL CODE SIGNAL TO SHIFT REGISTERS
90
DECODING LOGIC UNIT
80
SELECT CHAIN BUFFER
70
CLOCK/2

FIG. 1

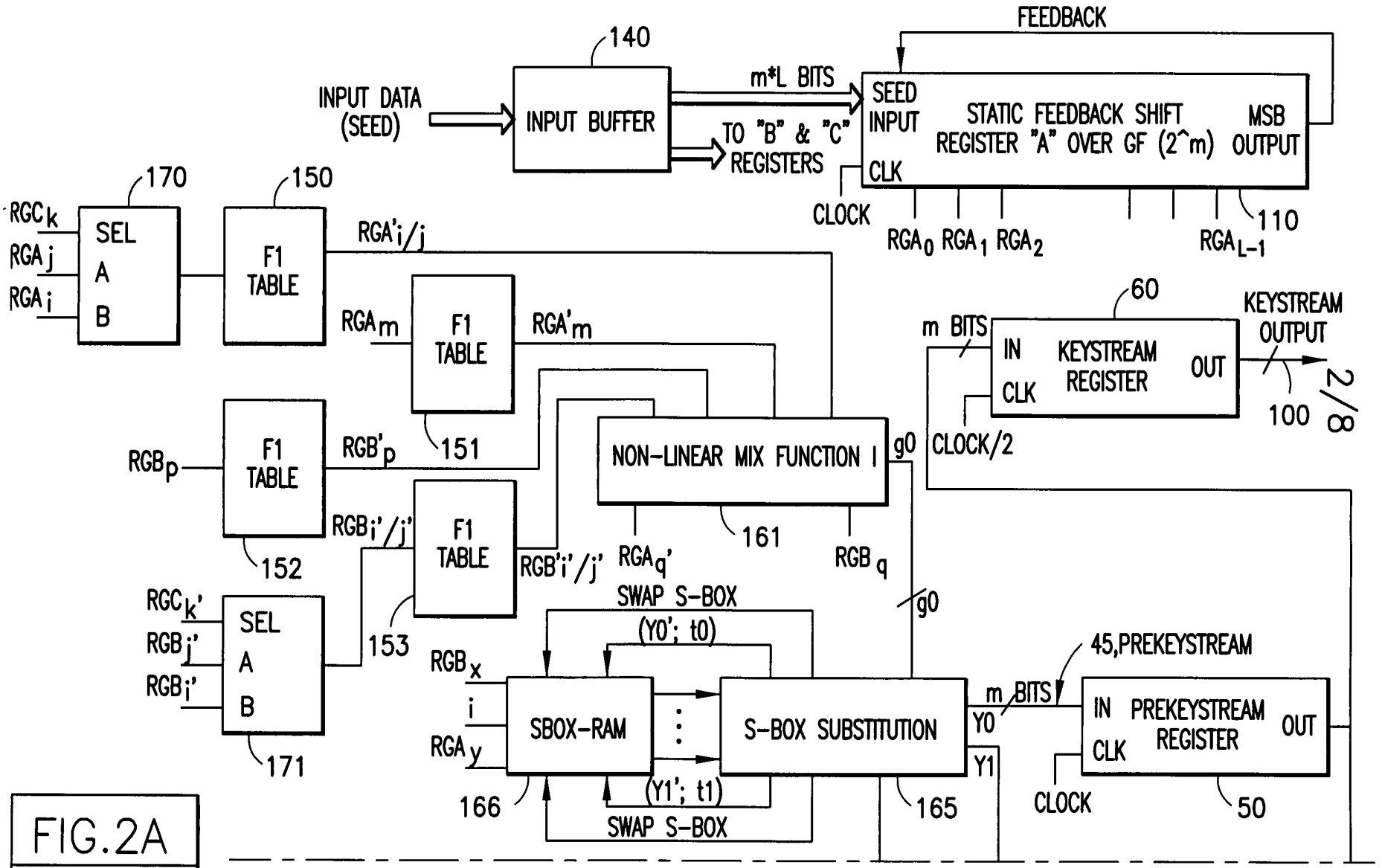

FIG.2A
FIG.2B

FIG.2

FIG.2A

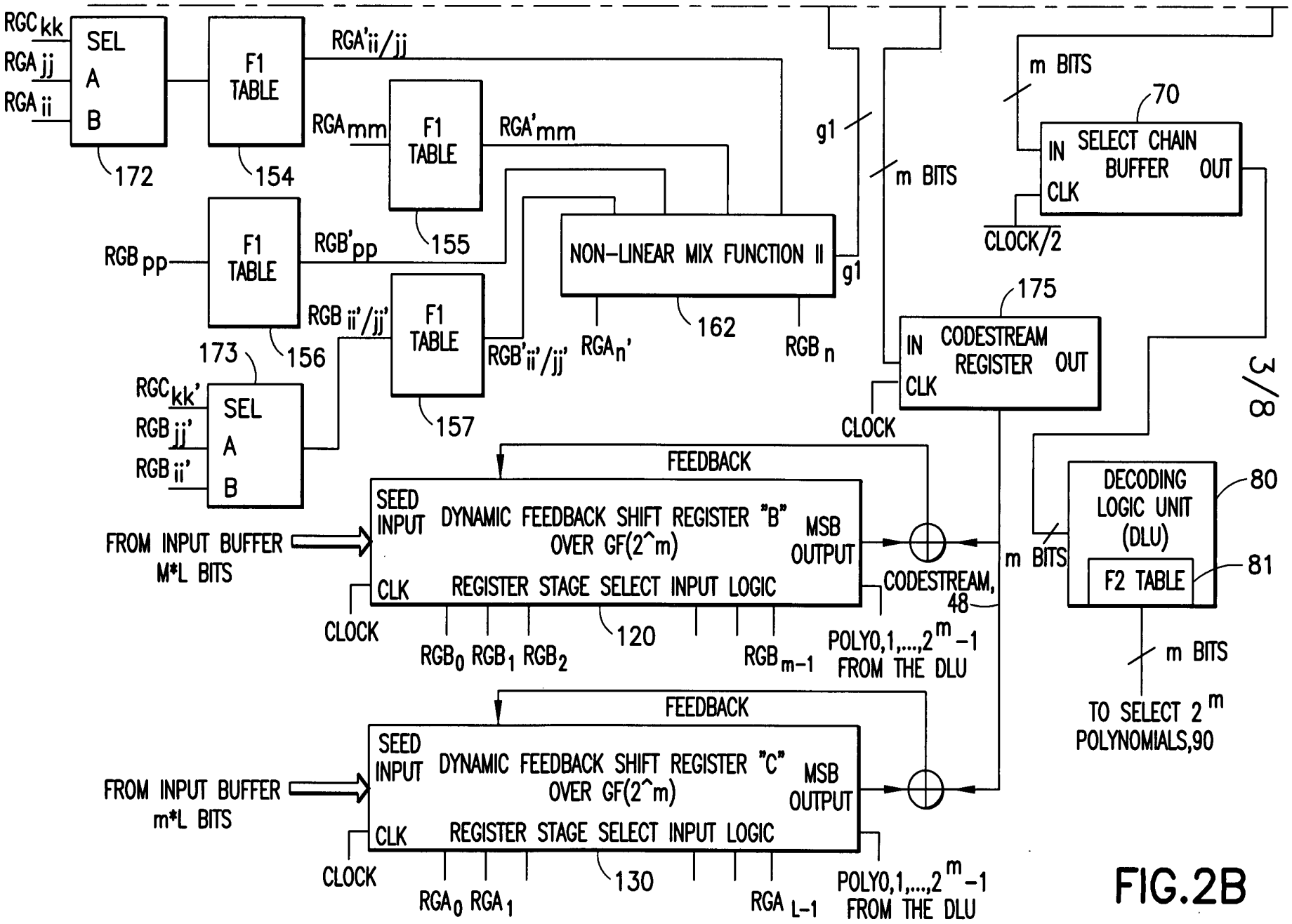
RGC kk
RGA jj
RGA ii
SEL
A
B
172
F1 TABLE
154
RGA'ii/jj
RGA mm
F1 TABLE
155
RGA'mm
g1
m BITS
m BITS
70
IN SELECT CHAIN BUFFER OUT
CLK
CLOCK/2
RGB pp
F1 TABLE
156
RGB'pp
NON-LINEAR MIX FUNCTION II
g1
RGB ii'/jj'
F1 TABLE
157
RGB'ii'/jj'
RGA n'
162
RGB n
175
IN CODESTREAM REGISTER OUT
CLK
CLOCK
173
RGC kk'
RGB jj'
RGB ii'
SEL
A
B
FEEDBACK
SEED INPUT
DYNAMIC FEEDBACK SHIFT REGISTER "B" OVER GF(2^m)
MSB OUTPUT
CLK
REGISTER STAGE SELECT INPUT LOGIC
FROM INPUT BUFFER M*L BITS
CLOCK
RGB0 RGB1 RGB2
120
RGB m-1
CODESTREAM, 48
POLY0,1,...,2^m-1 FROM THE DLU
m BITS
DECODING LOGIC UNIT (DLU)
80
F2 TABLE
81
m BITS
TO SELECT 2^m POLYNOMIALS,90
FEEDBACK
SEED INPUT
DYNAMIC FEEDBACK SHIFT REGISTER "C" OVER GF(2^m)
MSB OUTPUT
CLK
REGISTER STAGE SELECT INPUT LOGIC
FROM INPUT BUFFER m*L BITS
CLOCK
RGA0 RGA1
130
RGA L-1
POLY0,1,...,2^m-1 FROM THE DLU

FIG.2B

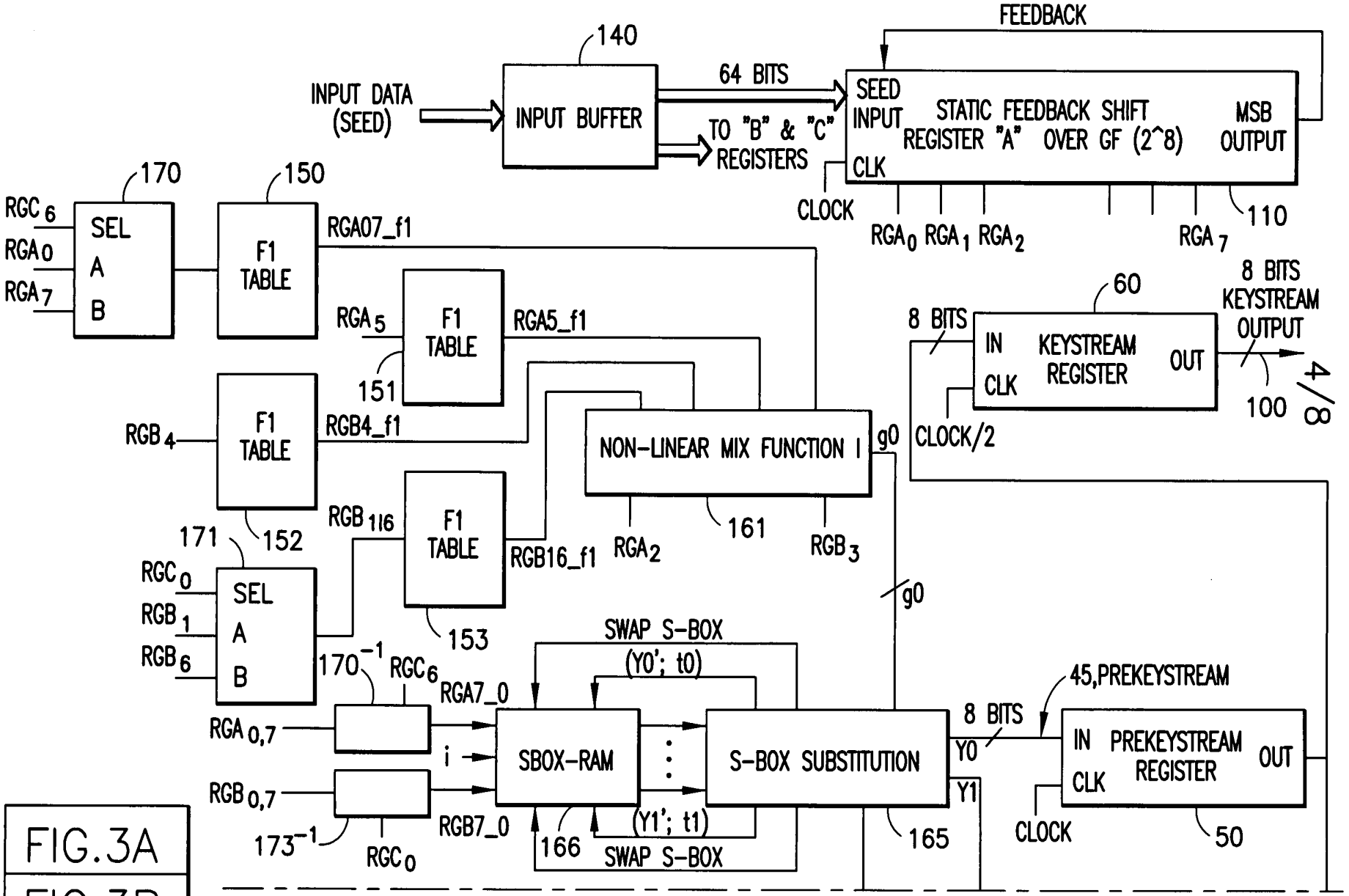

FIG.3A
FIG.3B

FIG.3

FIG.3A

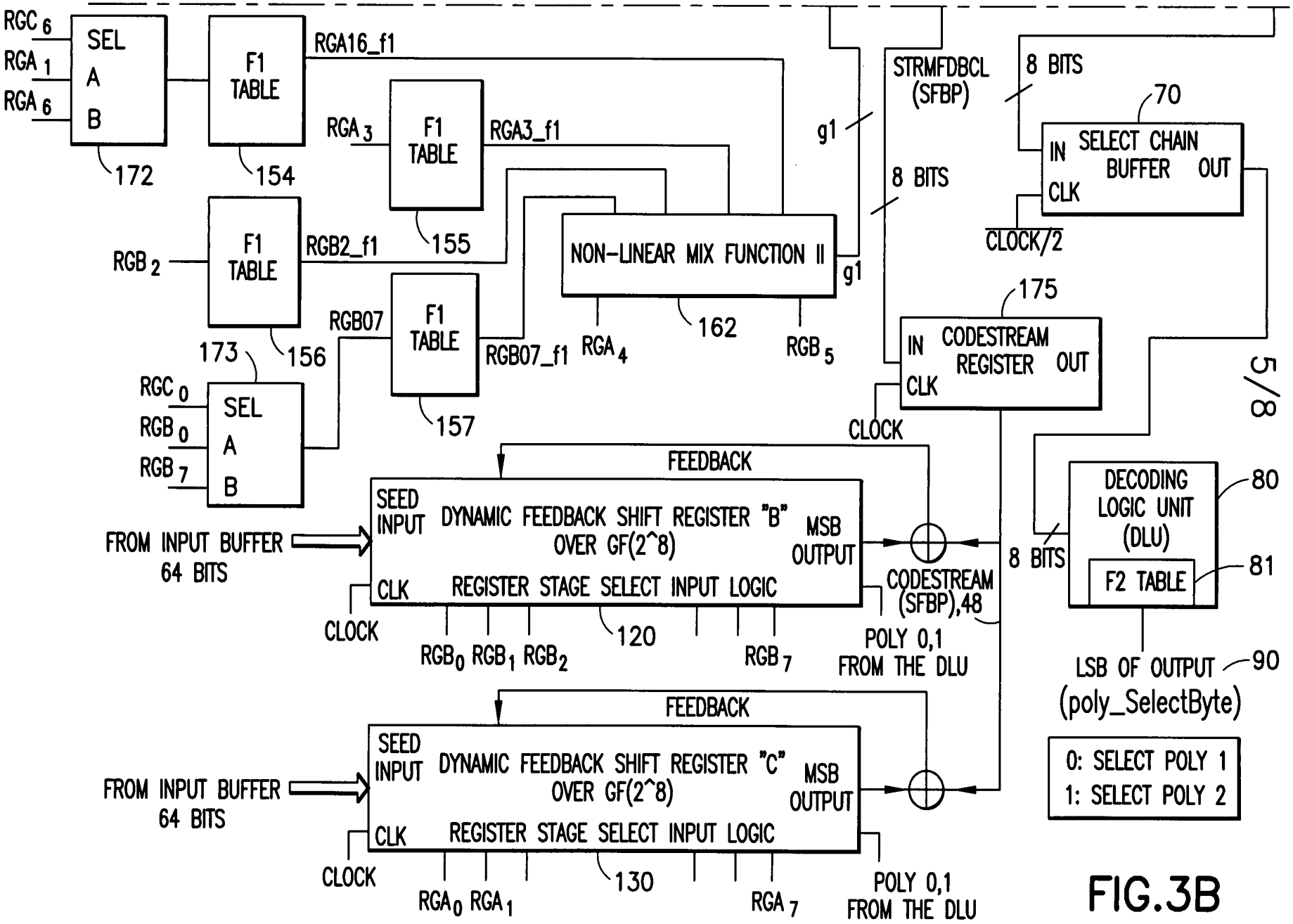
RGC 6
RGA 1
RGA 6
SEL
A
B
172
F1 TABLE
154
RGA16_f1
RGA 3
F1 TABLE
155
RGA3_f1
RGB 2
F1 TABLE
156
RGB2_f1
RGB07
F1 TABLE
157
RGB07_f1
173
RGC 0
RGB 0
RGB 7
SEL
A
B
NON-LINEAR MIX FUNCTION II
RGA 4
162
RGB 5
g1
g1
STRMFDBCL (SFBP)
8 BITS
8 BITS
70
IN SELECT CHAIN BUFFER OUT
CLK
CLOCK/2
175
IN CODESTREAM REGISTER OUT
CLK
CLOCK
FEEDBACK
SEED INPUT
DYNAMIC FEEDBACK SHIFT REGISTER "B" OVER GF(2^8)
MSB OUTPUT
CLK
REGISTER STAGE SELECT INPUT LOGIC
FROM INPUT BUFFER 64 BITS
CLOCK
RGB0 RGB1 RGB2
120
RGB 7
CODESTREAM (SFBP),48
POLY 0,1 FROM THE DLU
8 BITS
DECODING LOGIC UNIT (DLU)
80
F2 TABLE
81
LSB OF OUTPUT
90
(poly_SelectByte)
0: SELECT POLY 1
1: SELECT POLY 2
FEEDBACK
SEED INPUT
DYNAMIC FEEDBACK SHIFT REGISTER "C" OVER GF(2^8)
MSB OUTPUT
CLK
REGISTER STAGE SELECT INPUT LOGIC
FROM INPUT BUFFER 64 BITS
CLOCK
RGA0 RGA1
130
RGA 7
POLY 0,1 FROM THE DLU

FIG.3B

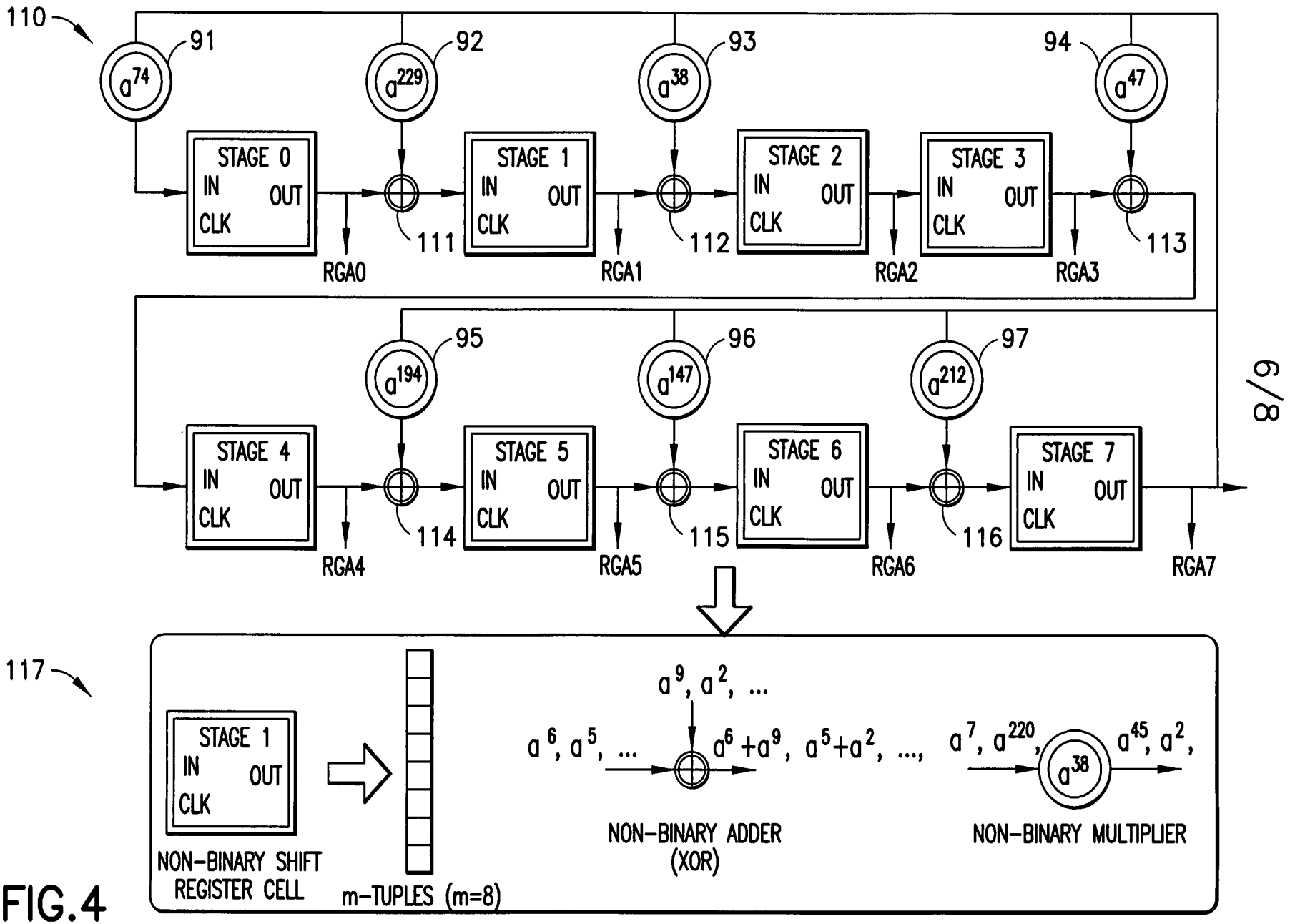
110
91
92
93
94
a^{74}
a^{229}
a^{38}
a^{47}
STAGE 0
STAGE 1
STAGE 2
STAGE 3
IN
OUT
CLK
RGA0
RGA1
RGA2
RGA3
111
112
113
95
96
97
a^{194}
a^{147}
a^{212}
STAGE 4
STAGE 5
STAGE 6
STAGE 7
RGA4
RGA5
RGA6
RGA7
114
115
116
117
STAGE 1
NON-BINARY SHIFT REGISTER CELL
m-TUPLES (m=8)
$a^9, a^2, \ldots$
$a^6, a^5, \ldots$
$a^6+a^9, a^5+a^2, \ldots,$
$a^7, a^{220},$
$a^{45}, a^2,$
a^{38}
NON-BINARY ADDER (XOR)
NON-BINARY MULTIPLIER

FIG.4

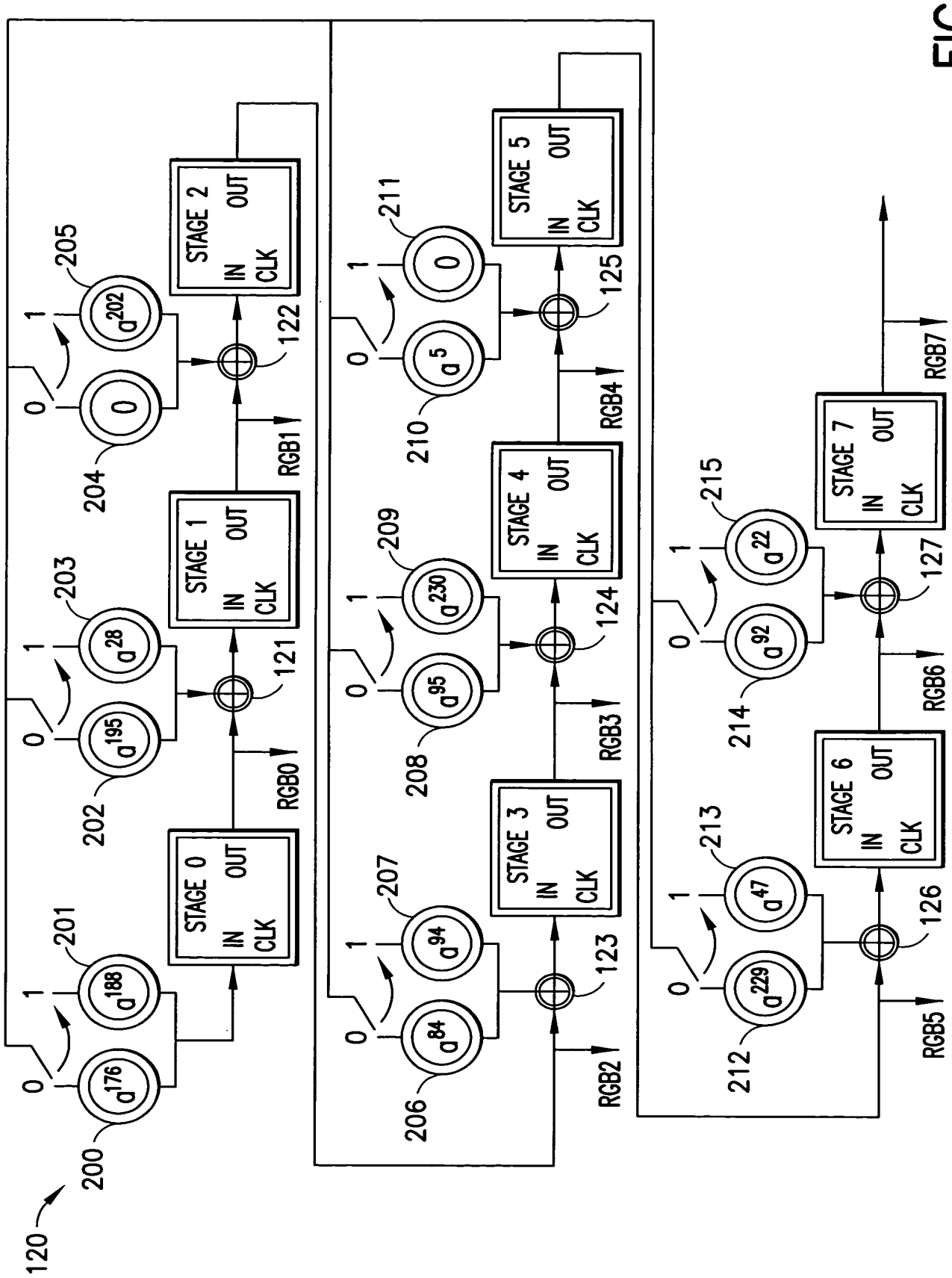
120
200
201
176
188
0
1
STAGE 0
IN
CLK
OUT
RGB0
202
195
203
28
121
STAGE 1
RGB1
204
0
205
202
122
STAGE 2
206
84
207
94
123
STAGE 3
RGB2
208
95
209
230
124
STAGE 4
RGB3
210
5
211
0
125
STAGE 5
RGB4
212
229
213
47
126
STAGE 6
RGB5
214
92
215
22
127
STAGE 7
RGB6
RGB7

FIG.5

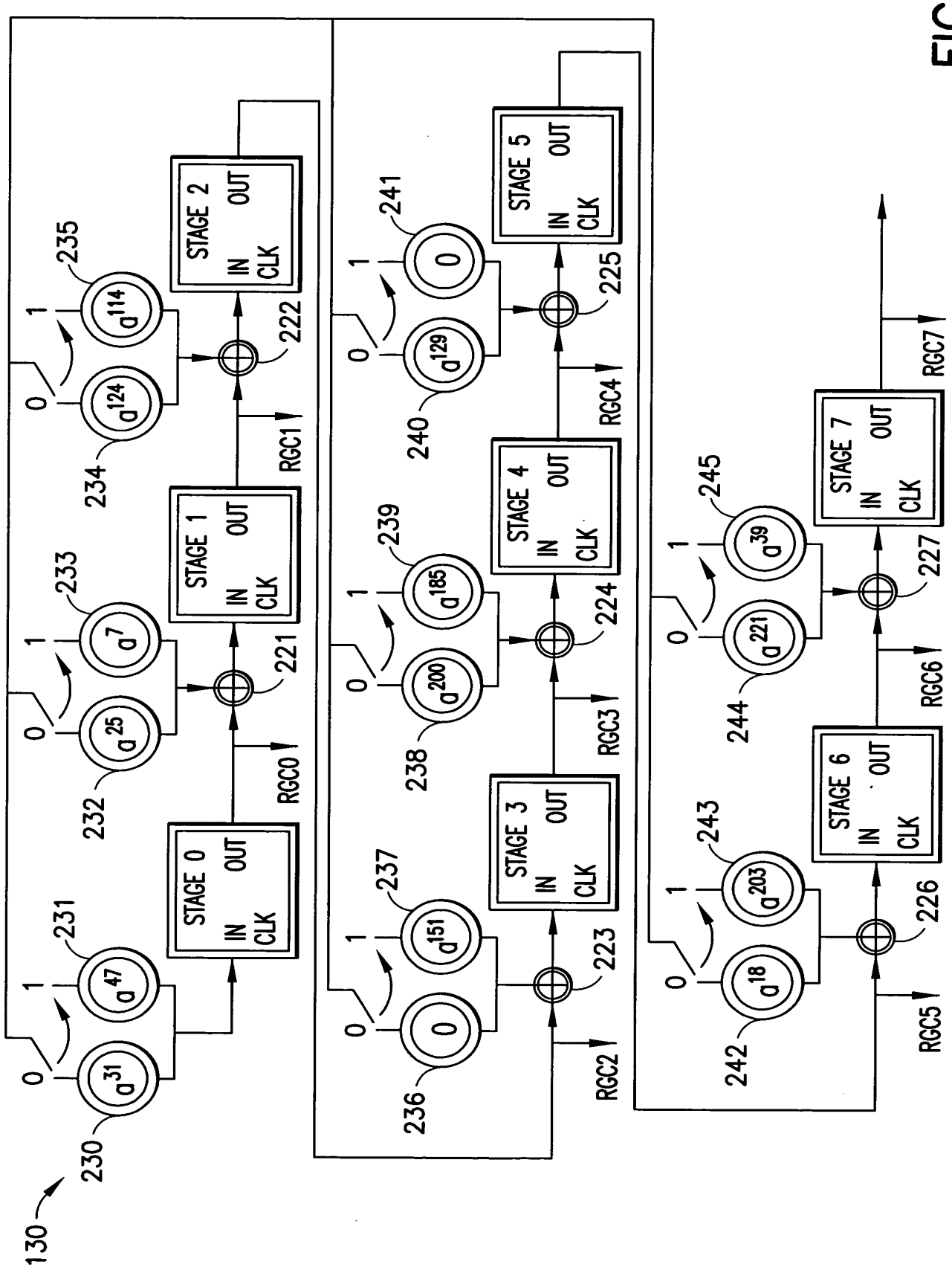
130
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
STAGE 0
STAGE 1
STAGE 2
STAGE 3
STAGE 4
STAGE 5
STAGE 6
STAGE 7
IN
OUT
CLK
RGC0
RGC1
RGC2
RGC3
RGC4
RGC5
RGC6
RGC7
221
222
223
224
225
226
227

FIG.6